

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1. Reed Elsevier is a world leading publisher of information for professional users focussed on three major market sectors, each of which is global. Reed Business is a provider of magazines, exhibitions, online media directories and marketing services across a diverse range of industries. Elsevier is a leading provider of science and health information serving 30 million scientists, students, health and information professionals. Lexis Nexis provides information and services solutions to professionals in the legal, risk management, corporate, government, law enforcement , accounting and academic markets.

Comments:

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2. The key benefits of sharing information are the social and economic benefits derived from enhanced efficiency, improved accuracy, avoidance of waste and duplication.

Appropriate use of information supports the prevention of crime in areas such as child abuse and the victimisation of mental patients and other vulnerable groups. Well managed information exchange supports the economy by facilitating speedy and transparent legitimate business activity and assisting in the prevention of fraud and other economic wrongdoing.

Comments:

Question 3. Properly conducted, information sharing is not a risk. As stated above, information sharing brings intrinsic social benefits through improved efficiency. It is only a risk when carried out irresponsibly.

Comments:

Question 4

Comments:

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments:

Question 8.

Comments:

Section 3: The legal framework

Question 9. We believe that in the electronic age the DPA framework may no longer be fit for purpose. The legislation should deliver privacy for the citizen without impairing the economic and societal benefits of data use. At present it is questionable whether that aim is achieved.

We suggest that conceptually the legislation could be refocused to permit multi purpose collection, storage and technical processing of data. The limitation to single purpose collection is a barrier to efficiency. It is not the act of collection and storage that causes harm. It is inappropriate use.

This loosening of restriction on collection, access and storage would need to be accompanied by a strengthening of provisions relating to loss of control of data - namely data breach. The philosophy would be that responsible_organisations should be permitted to collect and store databases of personal data (or to remotely access external databases from a central hub), and be authorised to enable appropriate_usage themselves or by responsible third parties. Lack of reasonable security leading to inappropriate usage would be subject to severe penalty.

The onus would be on the responsible data collector to verify the appropriateness of the third party receiving the data and its usage. Third party appropriateness would be determined by a combination of their identity (law enforcers, lawyers, risk professionals etc) and their intended declared use of the data.

Acceptable categories of user and acceptable uses of personal data could be defined by regulation. Some users or usage would require data subject consent either positive or negative, and some would be de jure, eg law enforcement. It would be a matter of open public debate which uses fell into which category.

Full data subject access provisions would be maintained and transparency increased.

The key to ensuring protection for the citizen is to switch focus from the activity of the processor to the impact on the citizen, to make the legislation citizen centric rather than processor centric. The key determinant would be the avoidance of damage to the citizen. Following through the logic outlined above, multi usage would be permitted by responsible organisations but the onus would be on the user of personal data to prevent harm in the course of that use. Organisations whose usage causes demonstrable harm could be subject to criminal and civil penalty.

Comments:

Question 10.

Comments:

Question 11.

Comments:

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments:

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments:

Question 21.

Comments:

Question 22.

Comments:

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:
